Patient Privacy and HIPAA/HITECH
What is HIPAA?

- **Health Insurance Portability and Accountability Act of 1996**
  - Implemented in 2003
- **Title II – Administrative Simplification**
- It’s a federal law
- HIPAA is mandatory, penalties apply for failure to comply
Purpose

- Protect health insurance coverage, improve access to healthcare
- Improve quality of healthcare in general
- Reduce Healthcare fraud and abuse
  - Set forth requirements regarding ensuring the privacy and security of protected health information (PHI)
- Reduce healthcare administrative costs (electronic transactions)
What is HITECH?

• Health Information Technology for Economic and Clinical Health Act

• Subtitle D of the American Recovery and Reinvestment Act of 2009 (ARRA)

• It’s a federal law
Purpose

- Makes massive changes to privacy and security laws
- Applies to covered entities and business associates
- Creates a nationwide electronic health record
- Increases penalties for privacy and security violations
Key HITECH Changes

- Breach Notification requirements
- AOD for treatment, payment, and healthcare operations in electronic health record (EHR) environment
- Business Associate Agreements
- Restrictions
- Right to Access
- Criminal Provisions
- Penalties
- OCR Privacy Audits
- Copy charges for providing copies from EHR
- HIPAA Preemption applies to new provisions
- Private cause of action
- Sharing of civil monetary penalties with harmed individuals
### Civil Penalties for Non-compliance*

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>All such violations of an identical provision in a calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not know</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect - Corrected</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect – Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

*As of 2/17/2009*
Criminal Penalties for Non-compliance

• For health plans, providers, clearinghouses and business associates that knowingly and improperly disclose information or obtain information under false pretenses. These penalties can apply to any “person”.
  • Penalties higher for actions designed to generate monetary gain
    – up to $50,000 and one year in prison for obtaining or disclosing protected health information
    – up to $100,000 and up to five years in prison for obtaining protected health information under “false pretenses”
    – up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm
Facility Privacy Official

• HIPAA requires healthcare entities to appoint a FPO. This appointment is made by the CEO.

• Que Le, RHIT (972-547-8142) is MCM’s FPO.

• Responsible for:
  – Privacy Program
  – Privacy Rights of patients
  – Requests for Privacy Restrictions
  – Facilitate training and education of staff
  – Compliance with requirements of the HIPAA Standards for Privacy
  – Ensure appropriate safeguards are in place to protect patient privacy
  – Receive Complaints about matters of patient privacy
HIPAA Terminology

- **HIPAA**: Health Insurance Portability and Accountability Act
- **HITECH**: Health Information Technology for Economic and Clinical Health Act
- **PHI**: Protected Health Information
- **CE**: Covered Entity (Hospital)
- **ACE**: Affiliated Covered Entity (Common Ownership)
- **OHCA**: Organized Health Care Arrangement (The hospital and medical staff will be considered an Organized Health Care Arrangement)
- **DRS**: Designated Record Set (medical record and billing record)
- **AOD**: Accounting of Disclosures (patient’s right to receive)
- **Directory**: Hospital Census list used by volunteers and operators with name and room
How will HIPAA and HITECH affect you?

• Patient information should only be accessed if there is a need to know (e.g., the information is required for the treatment of a patient, to carry out health care operations or for payment purposes). Only the minimum necessary amount of information may be used.

• Reasonable safeguards will need to be put into place for patient privacy protection

• Authorizations must be obtained from patient to release information for purposes such as health fairs, clergy, and services that vendors may provide on behalf of the patient
What is Protected by HIPAA (PHI)?

- Name
- Address including street, city, county, zip code and equivalent geocodes
- Name of relatives
- Name of employers
- Birth date
- Telephone numbers
- Fax numbers
- Electronic e-mail addresses
- Social Security Number
- Medical Record Number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Any vehicle or other device serial number
- Web Universal Resource Locator (URL)
- Internet Protocol (IP) address
- Finger or voice prints
- Photographic images
- Any other unique identifying number, characteristic, code

Each employee signs a Confidentiality and Security agreement, which states that information is not shared even after leaving HCA.
Notice of Privacy Practices

• Must be given to each patient that has face-to-face contact with hospital staff (e.g., inpatients, outpatients, health fair attendees)

• Must be acknowledged that the patient received the Notice

• Must be posted on website and in each of the registration areas of the facility
Confidential Communications

• Patients can request use of alternate address or phone number

• If there is a failure to respond by the patient, then we may revert to permanent address or phone number
Affiliated Covered Entity (ACE)

- Facilities in a shared clinical market (CPCS) and are under common ownership
- Members of the ACE must be documented
- All documentation maintained for 6 years
- Allows information to be shared between facilities in certain situations
Organized Health Care Arrangement (OHCA)

• Defined as a clinically integrated care setting in which individuals typically receive health care from more than one health care provider
  – This defines the relationship between the facility and the physician treating the same patient.

• Allows information to flow between the covered entities for treatment, payment, and health care operations without patient authorization
A complaint log must be maintained in accordance with the complaint process
Complaints must be investigated and documented with corrective action if applicable
Responses cannot be accompanied by retaliatory actions by the hospital
Disposition of complaint must be consistent with the facility’s Sanctions for Privacy Violations
Right to Privacy Restrictions

• Requests for such restrictions must be made in writing to the Facility Privacy Official (FPO)
• No other facility employee may process such a request unless specifically authorized by the FPO
• Requests may be denied
  – Example: “I don’t want my information shared with anyone outside the hospital.”
  • This would not be appropriate because information is required for state reporting and accreditation purposes (e.g., TJC)
Accounting of Disclosures

• Must provide documentation of certain disclosures of the designated record set for up to 6 years

• Examples
  – Medical and Billing Records
  – All required state reporting
  – Births and Deaths
  – Tumor registry reporting
  – Domestic/Child Abuse suspect reporting

• Very complex to implement

• Due to HITECH, additional requirements are forthcoming
Patient Rights

• Each patient is given a Notice of Privacy Practices
  – The patient signs an acknowledgement of receipt

• Right to Access
  – Patient has a right to inspect or obtain copies of their Medical and Billing Records
  – Any patient can access their medical records by stopping by HIM, showing ID, and filling out an authorization form.
• Right to access continued
  – Facility will provide a readable hard copy of portions of record requested
  – Patients can access any health information in our designated record set (DRS)
  – Patients that are still in-house have a right to access their information.
    • We encourage them to wait until discharge so their chart is complete.
    • If they insist, call HIM so that the request can be tracked appropriately and we can ensure all the appropriate information has been completed on the authorization.
    • If the patient wants to review the chart (no copies) this must be supervised.
– Requests may be denied under certain circumstances (i.e. the patient may cause harm to him or herself or others)

– Facility must respond to requests for access within 30 days or may send a letter to the patient stating issue and expected access or denial
Patient Rights continued

- Right to amend
  - Right to request an amendment of information within the Designated Record Set (DRS)
  - Request must be in writing and will not change or delete documentation, just amends
  - May deny the amendment with letter from the FPO
• Right to opt out of the directory

• Right to an Accounting of Disclosures

• Right to request to a privacy restriction of their PHI
  – Never agree to this, direct to FPO

• Right to confidential communication
Patient Directory

• The Directory kept by the PBX and information desk contains:
  – Patient Name
  – Room # / location
  – General condition
  • The diagnosis or procedure should never be disclosed.
• Patients listed as confidential are not listed.
• Patients have the option to opt out of the directory. When choosing to do this, they are not listed, and we do not acknowledge that they are here when asked.
How do I protect PHI?

• Authorizations are needed from patients to release information
  – Exception: We are allowed to release information without an authorization for Treatment, Payment, and Operations (TPO)
• Coversheets with Confidential statement needs to be used on all faxes (even if faxing within the hospital).
• Patients need to identify who their information can be discussed with, including family.
• Refrain from speaking about work specifics via electronic methods.
How do I protect PHI?

- Patient information is only accessed when there is a need to know. Never for curiosity!!!!
- Only the amount of information necessary is accessed.
- Computer screens need to be placed out of public view.
- Charts should not be left out where visitors can read the patient name or any documentation.
- All PHI is placed in a shred container when discarding. Never the trash!!!
- Conversations concerning patients should be made in private.
Electronic Communication

Remember that electronic communications are often not secure and information can be viewed or accessed by others without a need to know.

- Facebook
- Twitter
- Email
- Texting
Appropriate Releases or Breach of Confidentiality?

- PHI is discussed in a public place or with inappropriate individuals.
  - Inappropriate
- Physician views information for his/her patient
  - Appropriate
- Case Management shares information with a Nursing Home for patient placement.
  - Appropriate – for continuing care of the patient
- PHI was placed in the trash
  - Inappropriate
- TJC Reviewers access a chart.
  - Appropriate
Appropriate or Breach cont.

- Copy of electronic patient information is left exposed and unattended.
  - Inappropriate
- Viewing neighbor’s medical record because they won’t mind.
  - Inappropriate
- Viewing your own medical record
  - Inappropriate
- Quality of Care reviews.
  - Appropriate
- Physician views record for spouse that has been recently hospitalized
  - Inappropriate
HITECH provisions require the following notifications when breaches (as defined in the regulations) occur:
- To the patient
- To the Department of Health and Human Services
- To the media when the breach involves more than 500 individuals in the same state or jurisdiction
Ensuring Security Compliance

- Ensure users log off terminals when not in use.
- PC’s should have screen savers whenever possible.
- Computer screens should be positioned so information (PHI) is not readable by the public or other unauthorized viewers.
- Printers should be positioned in protected locations so that printed information is not accessible or viewable by an unauthorized person.
- PHI must be properly disposed.
Examples of Exposure

• Sharing of passwords

• Inappropriate control or use of patient lists with PHI

• Lack of knowledge regarding permitted uses of patient information

• Using business agents without contracts and appropriate Business Associate Agreements

• Discussing patient information on social networking sites (e.g., Facebook, Twitter)
Examples of Exposure

• Sharing PHI without an authorization when one is required

• Failure to act proactively to prevent, detect, or correct privacy or security breaches

• PHI in the trashcan

• Discussing PHI with someone who does not have a need to know
What happens when there is a violation?

• FPO must be notified

• FPO does investigation and classifies the violation as reportable or non-reportable
  – If non-reportable, education/discipline is conducted and the violation is tracked within the facility
  – If reportable, the violation is reported to corporate and HHS.

• Committee determines if violation must be reported to patient and/or public
Sanctions

• 3 levels of violations that require disciplinary action
  – Accidental and/or due to lack of proper education
  – Purposeful violation of privacy policy or an unacceptable number of previous violations
  – Purposeful violation of privacy policy with associated potential for patient harm
Final Notes

• MCM has a sanctions policy in place for violations.

• Refer any privacy complaints or questions to Que Le, RHIT, FPO.

• Now complete your post test and return to the student coordinator at MCM.